Government of India
Department of IT
National Informatics Centre
Cyber Security Division

Web site Security Audit
Request Form

Refer to Guidelines for filling up the Audit Request Form in Appendix – A.

1. Name of Web Site :

2. Name of Data Centre to be Hosted at :

3. URL of Web site :

Sl. No	URL of Web site	Temporary URL/ Staging Server URL	Comments
1.			
2.			

Aliases if any

4	**Alias URL(s) for the site on NICNET:(For ex: www.mnre.net, www.mnre.com)**	

Site Life span

5	**Nature of site (Tick one):**	**Event Based** ☐ **Permanent** ☐ **(Ex: A conference)**
6.	**If site is for an event provide the target date of GoLive/Hosting into Production**	

7. Whether copy of Web site made available in Cyber Security Division Lab **Y** ☐ **N** ☐

8. **Site Previously Audited and Certified Safe ?** **Y** ☐ **N** ☐

9. Application to be deployed in multiple departments ? (Ex: FTS, Intragov) **Y** ☐ **N** ☐

10. In the case that the site is an instance copy (without any changes/customizations/modifications) of an earlier audited site, then kindly provide the audited URL : ☐

11. Environment Details

a.	Operating System	

b.	Web Server (IIS/Apache)	
c.	Web applications details (asp, java, php, ISAPI etc.)	
d.	Database server details (MS Access, SQL server, Oracle, DB2)	
e.	Document details (HTML , pdf)	
f.	Website Type	Static ☐ Dynamic ☐ Cannot Determine ☐
g.	Type Project*	Paid ☐ Non-Paid ☐
h.	Development Base *	Third Party Development ☐ Developed by NIC ☐ NIC Coordinated Development ☐

* Audit requests for Paid Projects or Third Party developed web sites are not accepted by Cyber Security Division. Site owners are to audit their web sites thru CERT-In empanelled auditors**.**

12. Any Application(s) directory/URL not linked to the web site (For example: A site on staging URL http://demotemp59.nic.in/index.asp which has an Admin module or Content Management Module at http://demotemp59.nic.in/cms/ which is not directly linked from the web site at http://demotemp59.nic.in.) This URL may be provided here.

13. For web site requiring authentication (Basic, form based, certificate based) and different privileged access, provide two accounts in each role category.

Account Details :

Sl No	**Role**	**User Id**	**Password**	**User Id**	**Password**	**Authentication Basic/ Form/ if other state**
1.						
2.						
3						
4						
5						

Note : These accounts are to be strictly made available for audit purpose in order to test each of the role functionality. These are to be disabled or passwords changed in accordance with the password policy after the purpose is over.

14. Date of Submission of request :

15. Contact Details of NIC Personnel

a.	Name	
b.	Name of HOD	
c.	Division	
d.	Contact Telephone	
e.	Address	
f.	State	
f.	E-mail	
g.	Alternate E-Mail	
h.	HOD E-Mail	

16. Organisation originating request :

17. Contact Details of Organisation Personnel/ Site Owner

a.	Name	
b.	Name of HOD	
c.	Division	
d.	Contact Telephone	
e.	Address	
f.	State	
f.	E-mail	
g.	Alternate E-Mail	

18. Attached Documents :

1. Site Usage Policy Y☐ N ☐

19. Comments

Signature of HOD **Signature of Applicant**

Name : **Name of Applicant :**

Appendix – A

Guidelines for Filling up the Form.

1. **Name of Web site**: Provide the Name of the Web site.
2. **Name of Data Centre** to be Hosted at : Provide the name of the Data Centre where the site would be hosted. Ex: NIC, IDC, New Delhi, Lakshminagar Data Centre
3. **URL of Web site** : Provide the Production URL of the site. This would be the url of the site when hosted.

   Temporary URL/ Staging Server URL : Provide the temporary url or the staging server url where the copy of the site/application has been made available. This is where the tests would be conducted. Ensure that the url is functional before submitting the request.

   Comments : Any comments may be added here.
4. **Alias URL(s) for the site on NICNET** : If the site has multiple aliased URLs on NICNET such as for ex: www.mnre.net, www.mnre.com then these are to be provided here**.**
5. **Nature of site (Tick one):** Tick whether the site would be for an event such as a conference or exam results after which the site would be no longer required and may be taken offline. Or the site would be available for long term /permanently.
6. **If site is for an event provide the target date of GoLive/Hosting into Production:** In the case that the site is to be hosted for a conference then provide the target date by which the site would be required to be hosted.
7. **Whether copy of Web site made available in Cyber Security Division Lab** : If a copy of the site has been made available on the systems of Cyber security division lab then kindly state.
8. **Site Previously Audited and Certified Safe ?** State whether the site been ever audited earlier and certified safe.
9. **Application to be deployed in multiple departments ?** State whether the application is to be deployed in different departments/locations Ex: FTS (File tracking system) , Intragov sites etc.
10. **In the case that the site is an instance copy (without any changes/customizations/modifications) of an earlier audited site, then kindly provide the audited URL.** This field is to be provided in case of those sites which is an implementation copy of the a site as in 9. above. In this case you are to provide the url of the audited site. A separate document/certificate may be required in this case.
11. **Environment Details**
    a. **Operating System** : Provide the name of the OS such as Windows, Linux etc.
    b. **Web Server (IIS/Apache**) : Provide the name of the Web server such as IIS, Apache etc.
    c. **Web applications details** : Provide the type of application environment used in the site such as asp, asp.net, java, php, ISAPI etc.)
    d. **Database server details** : Provide the Database used such as MS Access, SQL server, Oracle, DB2, MySQL
    e. **Document details:** The type of documents hosted on the site such as HTML , pdf, .doc.
    f. **Website Type :** Provide the type of site such as Static or Dynamic. A static site hosts only static contents such as .html, .pdf, .doc .etc kind of pages. A dynamic site hosts

dynamic content generating pages and/or may include pages interactive pages. If you are not able to determine the nature of the site tick the option Cannot Determine

g. **Type Project :** State whether the site/application is developed as a part of Pias or Non – paid project. Audit requests for Paid Projects or Third Party developed web sites are not accepted by Cyber Security Division. Site owners are to audit their web sites thru CERT-In empanelled auditors and submit a security certificate at Cyber Security Division. Refer to guidelines for third party audit document at http://security.nic.in.

h. **Development Base :** State whether the site/application is a Third Party Development or developed by NIC or NIC Coordinated Development. Audit requests for Paid Projects or Third Party developed web sites are not accepted by Cyber Security Division. Site owners are to audit their web sites thru CERT-In empanelled auditors and submit a security certificate at Cyber Security Division. Refer to guidelines for third party audit document at http://security.nic.in.

12. **Any Application(s) directory/URL not linked to the web site:** Sometimes sites host applications which are directly not linked to the site. For example: A site on staging URL http://demotemp59.nic.in/index.asp which has an Admin module or Content Management Module at http://demotemp59.nic.in/cms/ which is not directly linked from the web site at http://demotemp59.nic.in. This URL may be provided here.

13. **For web site/applications requiring authentication** such as Basic, form based, certificate based etc with different roles/privileged access, provide two accounts in each role category. Ex:

    a. Role :manager invmgr/mnapwd1#, finmgr/mnapwd2

    b. Role: Customer cust1/sustpa@, cust2/pd1a$

    Note : These accounts are to be strictly tomade available for audit purpose in order to test each of the role functionality. These are to be disabled or passwords changed in accordance with the password policy after the audit purpose is over.

14. **Date of Submission of request** : Provide the Date of request submitted

15. **Contact Details of NIC Personnel** : Provide the contact details of NIC personnel coordinating/responsible for the site. This includes Name of contact, Name of HOD, Division, Contact Telephone, Address, State,E-mail, Alternate E-Mail, HOD E-Mail

16. **Organisation originating request** : Provide the name of the organization requesting the security audit for the site.

17**. Contact Details of Organisation Personnel/ Site Owner :** Provide the contact details of site owner including Name, Name of HOD, Division, Contact Telephone, Address, State, E-mail, Alternate E-Mail

18. **Attached Documents** : Kindly state about the attached documents such as Site Usage Policy. The site usage policy is to be provided for the application/site. The site usage policy typically states the purpose of the application/site. It includes the role of various site users/personnels and their privileges. Description about Information workflow is made in this document. Working data for test purpose are also provided in this document.

19. **Comments :** Provide any comments as or important instructions to be input that would be used during audit.